Altiris™ Software Management Solution 7.1 SP2 from Symantec™ Release Notes

Symantec™

Altiris™ Software Management Solution 7.1 SP2 from Symantec™ Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Altiris™ Software Management Solution 7.1 SP2 from Symantec™ Release Notes

This document includes the following topics:

About Software Management Solution

Altiris Software Management Solution from Symantec provides intelligent and bandwidth-sensitive distribution and management of software from a central

Web console. It significantly reduces desktop visits and lets you easily support your mobile work force. Software Management Solution also lets users directly download and install approved software, or request other software.

This product is part of the following suites:

- Altiris Client Management Suite from Symantec
- Altiris Server Management Suite from Symantec
- Altiris IT Management Suite from Symantec

What's new in Software Management Solution 7.1 SP2

In the 7.1 SP2 release of Software Management Solution, the following new features are introduced:

- Support of virtualization package format XPF.
  This enhancement ensures that the software catalog adds support of the default package format of Symantec™ Workspace Virtualization.
  For more information on XPF see topics on software virtualization in the *Software Management Solution User Guide* at the following URL:
  http://www.symantec.com/docs/DOC4661
- Added Mac support for certain **Run** settings in the Managed Software Delivery policy.
  The **Prompt user before running** and **Allow user to defer up to a total of options** in the **User run conditons** section of the **Run** setting in the Managed Software Delivery policy now support Mac.
  For more information on **User run conditions** for a Managed Software Delivery Policy see topics on Run settings in the *Software Management Solution User Guide* at the following URL:
  http://www.symantec.com/docs/DOC4661
- Microsoft Internet Explorer 6 support has been added for the Software Portal.

General installation and upgrade information

You install this product by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For more information, see the *Installing IT Management Suite* chapter in the *IT Management Suite 7.1 SP2 Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

See the product's documentation for information on how to configure and use it.

To perform an upgrade from version 7.1 or later, in the Symantec Installation Manager click **Install New Products**, and then choose to install this product. Do not use the **Install Product Updates** page to upgrade.

Symantec recommends that you upgrade all of the installed products to the latest version. The easiest way to achieve this is to choose to install a suite.

If you use hierarchy, you must disable hierarchy replication and upgrade all products to the latest version on each of the Notification Server computers.

For additional information about upgrading, see the **Upgrading to IT Management Suite 7.1 SP2 - Best Practices** article at the following URL:

http://www.symantec.com/docs/TECH177513

After you upgrade the product, you must upgrade the Symantec Management Agent and the plug-ins that are installed on the managed computers. Symantec recommends that you do the following:

- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the upgrade policies for the Symantec Management Agent.
- In the Symantec Management Console, click **Settings > All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for various site server plug-ins.
- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the upgrade policies for various plug-ins.

Symantec recommends that you configure a schedule for these policies; the default **Run once ASAP** option may not trigger the policy if this is not the first time you perform an upgrade. Also, to speed up the upgrade process, consider temporarily changing the **Download new configuration every** setting on the **Targeted Agent Settings** page to a lower value.

For detailed instructions on migrating from 6.x and 7.0 to 7.1 SP2, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.1 SP2* at the following URL:

http://www.symantec.com/docs/DOC4742

- *IT Management Suite Migration Guide version 7.0 to 7.1 SP2* at the following URL:
  http://www.symantec.com/docs/DOC4743

System requirements

Software Management Solution 7.1 SP2 requires the following software:

- Symantec Management Platform 7.1 SP2.

Supported platforms

The operating systems that are supported by IT Management Suite are also supported by Software Management Solution.

For more information, see the Symantec IT Management Suite Platform Support Matrix in the appendix of the *Altiris™ IT Management Suite from Symantec™ Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

In addition, Software Management Solution can manage the following server platforms that are not mentioned in the Symantec IT Management Suite Platform Support Matrix:

- Novell SUSE Linux Enterprise Server 11 SP1 - x64/x86
- Sun Solaris 10u9

For the operating systems that are supported by the Symantec Workspace Virtualization Agent 6.1 SP7 MR1 (6.4.1346) that is included in the product installation see the *Endpoint Virtualization Suite 6.1 SP7 MP1 Release Notes* at the following URL:

http://www.symantec.com/docs/DOC4600

Known issues

The following are known issues for this release. If additional information about an issue is available, the issue has a corresponding Article link.

For the most up-to-date information, latest workarounds, and other technical support information for this product, see the Technical Support knowledge base.

The known issues are separated into the following components:

- Installation and upgrade issues
  See Table 1-1 on page 7.
- Known issues
  See Table 1-2 on page 8.
- Hierarchy and replication issues
  See Table 1-3 on page 10.
- Managed Software Delivery issues
  See Table 1-4 on page 12.
- Software Portal issues
  See Table 1-5 on page 13.
- Virtualization issues
  See Table 1-6 on page 14.
- Non-Windows-specific issues
  See Table 1-7 on page 14.

Table 1-1 Installation and upgrade issues

Issue	Description	Article link
Added member accounts in the **Software Portal Administrators** and **Software Portal Managers** roles are not migrated from ITMS 7.0 MR4 to 7.1 SP2	Added member accounts in the **Software Portal Administrators** and **Software Portal Managers** roles are not migrated from ITMS 7.0 MR4 to 7.1 SP2. Workaround: After the migration is completed, you can manually add these member accounts to the **Software Portal Administrators** and **Software Portal Managers** roles.	N/A
Migrated sequential software delivery tasks can fail on clients however task shows exit code 0	A scheduled Managed Software Delivery policy that has been created using the Sequential Software Delivery Task from Software Delivery Solution can fail to run on target clients. However, on the clients where the policy has failed, the exit code 0 indicates that the policy was successful.	N/A
The Software Portal company logo settings do not migrate during off-box upgrade from Software Management Solution 7.0 SP2 to 7.1	The Software Portal company logo settings are reset to default after you perform migration from 7.0 SP2 to this version.	N/A

Table 1-1 Installation and upgrade issues *(continued)*

Issue	Description	Article link
Local users in software availability settings are lost after upgrade	When you migrate to 7.1, you install the Symantec Management Platform 7.1 to a new computer. The local users that you specified while configuring **Software Resource Availability** settings in software packages and managed delivery policies are no longer available after upgrade. The domain users and groups are migrated correctly.	N/A
Legacy task's WOL feature does not work	The Wake-on-LAN task is created for the legacy software delivery policies, but it does not work.	N/A

Table 1-2 Known issues

Issue	Description	Article link
The software delivery **Download Status** report incorrectly shows a "Success" status for a task which has failed to complete a package download.	The software delivery **Download Status** report incorrectly shows a "Success" status for a task which has failed to complete a package download. To find the **Download Status** report from the Symantec Management Console, on the **Reports** menu, click **All Reports**. In the left pane, click **Reports > Software > Delivery > Download Status**.	N/A
The **Policies to Include** drop-down list in the **Software Compliance Summary** report does not work.	When you select a policy to include from the **Policies to Include** drop-down list in the **Software Complaince Summary** report, data from the chosen policy should be shown. Instead no results are returned. Note: the **Computers to Include** down-list list does work correctly.	N/A
A Managed Software Delivery policy to unistall Microsoft Office 2007 fails with exit code 1603.	A Managed Software Delivery policy to unistall Microsoft Office 2007 fails with exit code 1603. Despite the exit code Microsoft Office 2007 does correctly uninstall.	N/A
Running Microsoft Active Directory Import overwrites any changes that are made to the pre-populated user details in the Software Portal.	Consider a domain user who changes pre-populated user details from the Active Directory on the **User Profile** page of the Software Portal. If the Microsoft Active Directory Import is run, these manual changes are overwritten by those from the Active Directory.	N/A

Table 1-2 Known issues *(continued)*

Issue	Description	Article link
Installing a policy's software into a virtual layer is not supported when SVS 2.1 is installed.	With a Managed Software Delivery, you can check the **Install this policy's software into a virtual layer** option. This option does not work when SVS 2.1 is installed on the client computer. You must have Symantec Workspace Virtualization 6.1 or later installed on the client computer.	N/A
Quick Delivery task timeouts if scheduled to run outside of maintenance window.	A Quick Delivery task fails to run if it is scheduled to run immediately, and the schedule is outside of a maintenance window. This issue occurs if a timeout period does not overlap with the maintenance window period. As a workaround, you can increase the timeout value or change the schedule.	N/A
Legacy software delivery tasks download their files to drive C.	The legacy software delivery tasks always download their files to drive C, even if the Symantec Management Agent is installed on another drive. For example, if the Agent is installed to `E:/mydir/`, legacy software delivery task's cache is created on `C:/mydir/` instead.	N/A
Compliance reports show incorrect data after solution reconfiguration.	If you reconfigure the solution through the Symantec Installation Manager, then compliance reports such as Software Compliance Status may show incorrect data.	N/A
The configuration of a **Quick Delivery** task can cause **Source Path Update** tasks and **Windows Installer Repair** tasks to fail.	When you install software with a **Quick Delivery** task, the MSI package is downloaded to and run on the client computer. In some cases, the way the **Quick Delivery** task is configured and installed can cause the **Source Path Update** task or the **Windows Installer Repair** task to fail. For more information, see knowledge base article TECH122112.	TECH122112
A software delivery task or policy installs the Wise Toolkit only for the user under which the installation runs.	When you create a software delivery task or policy to install Wise Toolkit and run it with the default settings, then Wise Toolkit items are not visible in the **Add or Remove programs** tool or **Start** menu for any user. Adding an option ALLUSERS=2 to the command line does not solve the problem. The reason is because the Wise Toolkit package is an EXE file and not an MSI file. Workaround: Set the **Run as** option of the task or policy to **Currently logged-on user**. Alternatively, set it to **Specific user** and specify the credentials of the user who use the Wise Toolkit on the computer.	N/A

Table 1-2 Known issues *(continued)*

Issue	Description	Article link
The Software Management Solution tasks do not support multicasting.	The Package Delivery, Quick Delivery, Source Path Update, and Windows Installer Repair tasks do not use multicasting. If you select the multicasting option in the global Symantec Management Agent settings, the multicasting does not occur.	N/A
When you assign permissions for a software resource on a parent domain, you cannot search for users and groups on a child domain.	When you publish a software resource to the Software Portal on a parent Notification Server computer, you cannot search for and select local users and groups of a child domain. You can assign permissions for the users and groups that are visible on the parent domain only. Workaround: The software publishing in hierarchy works properly when the parent Notification Server computer and its children are in the same domain.	N/A

Table 1-3 Hierarchy and replication issues

Issue	Description	Article link
Replication on a child Notification Server computer of an emergency policy update launched from a Managed Software Delivery policy with a Quick Delivery task does not work.	Consider a Managed Software Delivery policy containing a Quick Delivery task on a parent Notification Server computer. Specify targets to clients of the parent and clients of the child. Then launch the emergency policy update from this policy on the parent to the target clients on both the parent and child. The policy gets executed successfully on the clients of the parent Notification Server computer, but does not get replicated on the child Notification Server computer. An exception occurs in the Altiris Log Viewer stating that the policy does not have any package items associated with it.	N/A
The emergency policy update launched from a task you added in the Managed Delivery policy does not get replicated on child-level Notification Server computers.	The emergency policy update launched from a task you added in the Managed Delivery policy does not get replicated on child-level Notification Server computers. An exception occurs in Notification Server logs stating "does not have any package items associated with it".	N/A
Modified detection rule does not replicate when you use the **Replicate Now** option.	Consider a Managed Software Delivery policy that has been replicated to a child Notification Server. If the detection rule in the policy is modified, then these changes are not replicated to the child using the **Replicate Now** option. Note that these changes are correctly replicated to the child when you use a differential replication schedule. For more information, see topics on hierarchy configuration in the *Symantec Management Platform Help*	N/A

Table 1-3 Hierarchy and replication issues *(continued)*

Issue	Description	Article link
Policies with **Power on computers if necessary** option do not work correctly on child.	Consider any Managed software delivery policies that have the **Power on computers if necessary (using Wake-on-LAN, Intel AMT, ASF or DASH)** option checked. Under such settings, the policies do not turn on the computers when run from the child Notification Server. Workaround: On the child Notification Server, open the replicated policy and click **Save changes**. This action recreates the power management task.	N/A
The Software Delivery task or policy execution event data is not replicated up the hierarchy by default.	The replication of the Software Delivery task or policy execution event data is disabled by default. As a result, the Software Management Solution reports on a parent Notification Server do not show any information from the child Notification Servers. To view the reports from the child Notification Servers on the parent Notification Server, you must enable the following data classes for replication: ■ **AeX SWD Execution** ■ **AeX SWD Package** ■ **AeX SWD Status** To enable the replication of the data classes: 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**. 2 In the right pane, on the **Hierarchy Management** page, on the **Replication** tab, under **Events**, check the **Software Package and Delivery Event Replication Rule**. **Note:** In some large environments, the enablement of these data classes can have an affect on the performance of the parent Notification Server. It is recommended you evaluate the effect on performance before the full-scale rollout.	N/A

Table 1-3 Hierarchy and replication issues *(continued)*

Issue	Description	Article link
Software Portal requests from a child Notification Server computer cannot be managed from the parent server.	Software Portal requests do not replicate up the hierarchy from the clients of a child Notification Server . As a result, those requests cannot be processed from the parent Notification Server in a global hierarchy scenario. Workaround: Software Portal requests on a child Notification Server can be processed in either of the following ways: ■ The administrator of the child Notification Server can process and manage the requests. ■ The administrator of the parent Notification Server can assign users or groups to the Software Portal manager role. Anyone who has the Software Portal manager role can process and manage the requests from the Software Portal Manager page on the child server.	N/A
Replication of the Software Portal company logo settings is not possible.	When you specify Software Portal settings on a parent Notification Server and want to replicate these settings to its children, not all data is replicated. The company logo is not replicated because it is a physical file that is stored on the parent Notification Server. You cannot replicate physical files. Workaround: You can manually replace the `SymantecLogo.png` image file on the child Notification Server computer, in the `C:\Program files\Altiris\Software Management Solution\Software Portal\Web\Images` folder.	N/A
The Software Portal user rights of the local users do not replicate properly from the parent Notification Server computer to its children.	The Software Portal user rights of the local users do not replicate properly from the parent Notification Server computer to its children. This problem does not occur for the domain user accounts and user groups.	N/A

Table 1-4 Managed software delivery issues

Issue	Description	Article link
A Managed Software Delivery policy does not start when you add a compliance schedule **At user login** and a defined **End date**.	A Managed Software Delivery policy does not start when you add a compliance schedule **At user login** and a defined **End date**. For more information, see the topics on specifying a policy schedule in the *Symantec Management Platform User Guide* at the following URL: http://www.symantec.com/docs/DOC4730	N/A

Table 1-4 Managed software delivery issues *(continued)*

Issue	Description	Article link
A Managed Software Delivery policy containing **Power Management** task does not deliver to the target computer.	A Managed Software Delivery policy containing a **Power Management** task does not deliver to the target computer. The policy does save successfully, however an information message appears which explains this issue. The message reads as follows: "[X] resources are automatically excluded and not shown in the policy because they are not capable of running one or more tasks selected in the policy (see Altiris log for details about the tasks names). The policy will not be delivered to those resources. Consider removing the tasks that are causing this limitation." Workaround: Remove the **Power Management** task from the policy to ensure that the affected resources can be delivered.	N/A
Problems occur when you delete a Managed Software Delivery policy that is published in the Software Portal.	When you delete a Managed Software Delivery policy that is published in the Software Portal, the following problems appear: ■ You cannot select and delete multiple Managed Software Delivery policies at once. You must select a single Managed Software Delivery policy, delete its item references, and then delete the policy. ■ When you delete an item reference of a Managed Software Delivery policy, the **Item References** list is not automatically refreshed. You must refresh the **Item References** list manually to see which of the items have been deleted.	N/A

Table 1-5 Software Portal issues

Issue	Description	Article link
Software Portal does not work with Safari 4.0.4 for Windows Web browser or later.	If you access the Software Portal using Safari 4.0.4 for Windows Web browser or later, some of the functionality does not work. Safari incorrectly processes postbacks from the controls that require server-side handler execution during postbacks. In addition, the Software Portal Shortcut on the desktop does not display a user credentials prompt. Instead the Software Portal opens under the credentials of the user who last logged into the system.	N/A
User must refresh the desktop for the Software Portal shortcut to appear.	If the Software Portal plug-in has been installed, the desktop shortcut does not appear until the desktop is refreshed.	N/A

Table 1-5 Software Portal issues *(continued)*

Issue	Description	Article link
Software Portal fails to load if Notification Server is moved from workgroup to a domain.	If you join the Notification Server computer to a domain, the Software Portal page becomes inaccessible. Workaround: Configure the Notification Server computer Application Identity account with the domain administrator account. Make sure that this account also has access to the database.	N/A
Some filters do not work as expected.	The **Approved Software** and **Approved Managed Delivery** filters in the administrator's portal do not include pre-approved software that did not require an administrator's approval. Use the **All Approved** filter if you want to view both pre-approved software and the software requests that are approved by an administrator.	N/A

Table 1-6 Virtualization issues

Issue	Description	Article link
To successfully accomplish a Software Virtualization Command task that imports a vsa file, you must specify the same layer name that the vsa file contains.	When you want to create a Software Virtualization Command task that imports a vsa file, you must specify a layer name. The problem is that the vsa file already contains a layer name; therefore, specifying it once more should not be necessary. Furthermore, when you specify a different layer name, the Software Virtualization import task fails. Workaround: Find out the layer name that the vsa file contains and type it in the **Create new task** dialog box, in the **Layer name** box.	N/A
When you install software into a virtual software layer with a localized layer name, the localized name does not appear in the SVS Admin on the client computer.	In a Managed Delivery policy, if you choose to virtualize the software during installation, you must provide a name for the virtual layer. If you enter a localized string as the layer name, the software appears in the SVS Admin with the default layer name **SWD** instead of the localized layer name that you provided.	N/A

Table 1-7 Non-Windows-specific issues

Issue	Description	Article link
The **Execution Attempts** report shows two entries for one task.	When you run a Quick Delivery task on a UNIX/Linux/Mac computer, two entries appear in the **Execution Attempts** report. One entry has the task name and the other has the name of the executed command line.	N/A

Table 1-7 Non-Windows-specific issues *(continued)*

Issue	Description	Article link
Quick Delivery package download incorrectly reported as failed.	When a Quick Delivery package is downloaded to the client successfully, but the task failed to run, the package download status is shown as **Failed** in the **Download Status** report. You can ignore this error.	N/A
Some Managed Software Delivery settings do not work for non-Windows computers.	The following Managed Software Delivery settings do not apply to UNIX, Linux, or Mac delivery policies: ■ **Power on if necessary (using Wake-On-LAN, Intel AMT, ASF, DASH)** Appears on the **Managed Delivery Settings** page, on the **Schedule** tab, under the **Compliance** section. ■ **Only perform check if... Computer is available at the exact scheduled time** Appears on the **Managed Delivery Settings** page, on the **Schedule** tab, when you click the **Advanced** button. ■ **Upon success run** Appears on the **Managed Delivery Settings** page, on the **Run** tab, under the **Results-based actions** section.	N/A
You cannot execute Managed Software Delivery policies from the client side on non-Windows computers.	The client-side user interface (on the Symantec Management Agent) is not available on UNIX, Linux, or Mac computers. Therefore, you cannot execute Managed Software Delivery policies from those client computers. This issue occurs because those policies do not appear in the utility "aex-swdapm" on UNIX, Linux, or Mac clients.	N/A
A Managed Software Delivery upgrade of a Linux RMP package does not work.	A Managed Software Delivery upgrade of an rpm package does not work due to limitations of the rpm detection rules. When a policy with the rpm command is delivered to the UNIX, Linux, and Mac agent, the detection rules look for software resources with the same version as the software resource in the policy, instead of a previous version of the software resource. Consequently, a previous version of the software resource is not detected and the upgrade does not execute. A workaround is to use a Quick Delivery or a Package Delivery task for the upgrade because they do not use detection rules. You can also edit the detection rule of the software resource on the **Rules** tab in the Software Catalog. Change the **Status** field of the rule from the default value of EQUAL to LESS so that the detection rule looks for a previous version of the software resource.	N/A

Table 1-7 Non-Windows-specific issues *(continued)*

Issue	Description	Article link
Keys generation for depot files is broken. Only the package name is available that is used as a key during the import process (without any operating system name or architecture).	Some UNIX, Linux, and Mac software packages not containing architecture and supported operating system version information may be detected during import as the same package. Workaround: Rename one of the conflicting packages.	N/A
Managed delivery policy does not detect already installed software when it is delivered in archived format.	After software is delivered in archived format, the ULM agent cannot track the installed software but can only track the archived package. Software is only marked as uninstalled after you generate the uninstall type command for the same software package and schedule it to the client.	N/A
The **Allow user to interact with installing software** option does not function on Mac operating system.	When you set this option as part of a Managed Software Delivery for Mac, the option does not work. The notification pop-up may appear (if you are logged into the shell), but it is non-functional.	N/A
RTE Command Line Builder generates an incorrect install command.	When you manually create a software package that contains .rte files and use RTE Command Line Builder to generate the appropriate installation command line, the package installation may fail. The command line is the command to execute the installation file on client systems. This failure can occur because the generated command line contains the %SIFNAME% token. This token is added as a part of the command and is not replaced on the client system with the software installation file name. This issue results in a failing installation of the software on client systems. For manually created packages containing .rte files, replace the %SIFNAME% token with the appropriate file name.	TECH46206
Agent does not load user's environment variables when software delivery jobs are executed under non-root user.	Task fails when running software delivery in Mac UI under currently logged-in user. The user was logged as "tester" (not root) and "Run Task" button was pressed under Utilities -> Altiris Agent -> Software Delivery. Command line was used as : `whoami >> $HOME/task1.log` The result was not written in appropriate directory and history showed an error. Running "aex-swdapm" from command-line did not reproduce this error. Command was run successfully and result written to $HOME/task1.log file. This also applies for Run as option in advanced option of software delivery policy.	N/A

Table 1-7 Non-Windows-specific issues *(continued)*

Issue	Description	Article link
Advanced Run Options and **User run** conditions options for Package Delivery, Quick Delivery , and Managed Software Delivery do not function.	Mac/ Tasks/ Advanced Run Options - User run conditions do not function. Steps to Reproduce: Scenario 1: Task can can only when user is logged on 1 Click **Manage > Jobs and Tasks > Samples > Remote Management > pcAnywhere Plug-in install task for Mac**. 2 Click **Advanced > Run Options**. 3 Select Symantec Management Agent credential OR specify a user by entering the Domain, User name, Password and Confirm password. 4 In the User run conditions, Task can run: - Only when user is logged on. 5 Click **OK > Save changes.** 6 In Quick Run, select the desired Mac host and click **Run**. Keep the Mac host is in logged OFF state. Result: pcA plugin is found to be installed. Scenario 2: Task can run only when user is not logged on 1 Click **Manage > Jobs and Tasks > Samples > Remote Management > pcAnywhere Plug-in install task for Mac**. 2 Click **Advanced > Run Options**. 3 Select Symantec Management Agent credential OR specify a user by entering the Domain, User name, Password and Confirm password. 4 In the User run conditions, Task can run: - Only when user is not logged on. 5 Click **OK > Save changes**. 6 Keep the Mac host in logged on state with the specified user. 7 In Quick Run - select the desired Mac host and click on Run. Result: pcA plugin is installed.	N/A
The Software Management Agent for Mac does not support asynchronous deferring of software delivery jobs.	Currently Mac OS does not support multiple software delivery jobs deferring at the same time from UI. If two or more jobs arrive to the client, a user can defer only the first one. All others need to wait until the first job is executed.	N/A

Fixed issues

The following are the previous issues that were fixed in this release. If additional information about an issue is available, the issue has a corresponding Article link.

Table 1-8 Fixed issues

Issue	Description	Article link
A lot of deadlocks can appear when several users make a request from the Software Portal.	`Errors occur while processing software portal page` errors and deadlocks appear when several users make requests for Managed Software Delivery policies from the Software Portal. Improved Software Portal stability is required when many users make requests simultaneously.	N/A
Managed Software Delivery Policy targets created by the Software Portal are not excluded from replication even when HEP is enabled for resource targets.	Managed Software Delivery Policy targets created by the Software Portal are not excluded from replication even when HEP is enabled for resource targets. It should be not required to have the HEP option enabled for Managed Software Delivery policies that are published to the Software Portal in a hierarchical environment.	N/A
A Quick Delivery task can be slow to load.	A delay of up to 4 seconds can occur when you try to load a Quick Delivery task in the Symantec Management Console. As a consequence, changes are required to improve the performance of the Quick Delivery task loading time.	N/A
The Software Portal can open slowly if you try to log in with very large numbers of software published.	If you open the Software Portal with very large numbers of software published it can take up to 90 seconds for the page to load.	N/A
A Managed Software Delivery policy that uses the **Restart Computer** task can fail to initiate a computer restart.	A Managed Software Delivery policy that uses the **Restart Computer** task can fail to initiate a computer restart. In addition, when the restart is initiated correctly, the Symantec Management Agent can indicate a failure.	N/A
A Managed Software Delivery policy does not work under certain scheduling settings.	A Managed Software Delivery policy does not work properly when you use the following scheduling settings: ■ **Computer is available at the exact scheduled time** compliance schedule and remediation schedule are both selected. ■ The **End** date is already passed when the policy is evaluated.	N/A

Table 1-8 Fixed issues *(continued)*

Issue	Description	Article link
Registry inventory rules do not support checking `HKEY_CURRENT_USER` when the **Run As** option is used in a Managed Software Delivery policy.	A Managed Software Delivery policy does not respect the **Advanced Options > Run > Run As** settings when a software resource uses **Applicability** or **Detection** rules. These rules should use the user registry and user-specific known folders when the **Currently logged-on user** or **Specific user** options are selected.	N/A
Sometimes **Virtualized Software Resources** reports do not show all the data.	Sometimes **Virtualized Software Resources** reports can show incomplete data relating to the operations with virtualized software. Evaluation results for a managed software delivery policy that is installed into a virtual layer are also absent from the **Virtualized Software Resources, Compliance, and Delivery** reports. The issue can occur on Microsoft Windows Vista, 7 and 2008 operating systems.	N/A
Keep **Resource target** property enabled for some policies.	If you publish a managed software delivery policy to the Software Portal on the child Notification Server, you must keep the **Resource target** property checked.	N/A
Microsoft Internet Explorer 6 is not supported.	Software Portal does not work with Microsoft Internet Explorer version 6.	N/A
Error appears when you assign 6.x software delivery packages to software resources.	If you select a large number of software delivery packages and select the **Action > Assign to Software Resources** right-click action, an error can be displayed. Workaround: select a smaller number of packages.	N/A
Except for Application Management, Portal and Virtualized Software Resources reports, reports scoping does not work for Software Management Solution reports.	Except for Application Management, Portal and Virtualized Software Resources reports, reports scoping does not work for Software Management Solution reports.	TECH160947

Table 1-8 Fixed issues *(continued)*

Issue	Description	Article link
During a Managed Software Delivery Policy requesting `SqlException: Violation of PRIMARY KEY constraint 'PK_TargetFilterResource'. Cannot insert duplicate key in object 'dbo.TargetFilterResource'` is logged to Notification Server log and policy cannot be made in **approved** state.	During a Managed Software Delivery Policy requesting `SqlException: Violation of PRIMARY KEY constraint 'PK_TargetFilterResource'. Cannot insert duplicate key in object 'dbo.TargetFilterResource'` is logged to Notification Server log and policy cannot be made in **approved** state. This issue is only valid for migrated from 7.x policies which are already requested in the 7.x environment and approved. Consider a scenario when an upgrade is performed and policy targets are deleted for these migrated policies. This issue appears for the clients that have already requested this policy or for those clients that request this policy for the first time. This situation may also happen if Hierarchy is set up and during policy replication HEP controls are disabled. After replication is done, policy targets are deleted and after you try to request it once again this situation appears.	TECH160945
A managed software delivery policy that is targeted for a user to deliver a task does not arrive to the client computer.	A managed software delivery policy that is targeted for a user to deliver a task does not get to the client computer. The policy does not get delivered to the client even after a client log-in is performed. In addition, when you save the policy for the first time the number of resources in **Applied to** tab is correct. However if you reopen the policy or click **Save** again the **Applied To** is set to `0` resources even though the target is present.	N/A
In certain conditions, the managed delivery policy compliance status can be incorrect.	The compliance status of a managed software delivery policy can be incorrect in the following scenario: 1 Software resource B follows Task A 2 The **Upon failure the Managed Delivery will** option for Task A is set to **Continue**. 3 When the managed software delivery policy runs on the client computer, task A fails, and the software resource B succeeds.	N/A
The **Show link for Software Portal in Start Menu** option is non-functional.	The **Show link for Software Portal in Start Menu** option on the **Software Portal Plug-in Policy** page is non-functional. No link is created on the client computer. Workaround: Create a **Symantec** subfolder in the **Start** menu and then reapply the policy.	N/A

Table 1-8 Fixed issues *(continued)*

Issue	Description	Article link
Software Portal managed users are not replicated to child.	Users that are assigned to a Software Portal manager are not replicated to the child Notification Servers. As a result, the software requests go to the Software Portal administrator instead of the manager. To work around this issue do the following: **1** Add users to the Software Portal manager's direct reports list on the child Notification Server manually. **2** Approve the Software Portal requests on the child Notification Server. **3** On the parent Notification Server, publish pre-approved software to the Software Portal.	N/A
Published managed delivery policy cannot be edited and executed on child.	The managed software delivery policies that are published to the Software Portal and then replicated cannot be edited and executed on the child Notification Server. This issue occurs even if the **Hierarchy Editable Properties** settings allow editing. You can do one of the following to work around this issue: ■ Edit the policy on the parent Notification Server. ■ Clone the policy on the child and edit the cloned policy.	N/A

Other things to know

There are no other things to know in this release.

Documentation that is installed

Table 1-9 Documentation that is included in the product installation

Document	Description	Location
Help	Information about how to use this product. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. To open context-sensitive help, click inside the window, pane, dialog box, or other screen element about which you want more information, and then do one of the following: ■ Press the F1 key. ■ In the Symantec Management Console, click **Help > Context**. In the **Symantec Help Center** window, type your search string to search within the installed documentation. To expand your search to the Symantec Knowledge Base, check **Include online search**. For more information on how to use the **Symantec Help Center**, click the **Home** symbol.
User Guide	Information about how to use this product. This information is available in PDF format.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. The Documentation Library provides a link to the PDF User Guide on the Symantec support Web site. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.

Other information

Table 1-10 Information resources that you can use to get more information

Document	Description	Location
ITMS 7.1 SP2 Planning and Implementation Guide	Information about capacity recommendations, design models, scenarios, test results, and optimization best practices to consider when planning or customizing ITMS.	http://www.symantec.com/docs/DOC4827

Table 1-10 Information resources that you can use to get more information *(continued)*

Document	Description	Location
Symantec Management Platform User Guide	Information about using the Symantec Management Platform.	Symantec Management Platform Documentation page
Symantec Management Platform Release Notes	Information about new features and important issues in the Symantec Management Platform.	Symantec Management Platform Documentation page
Symantec Management Platform Installation Guide	Information about using Symantec Installation Manager to install the Symantec Management Platform products.	http://www.symantec.com/docs/DOC4798
Knowledge base	Articles, incidents, and issues about this product.	SymWISE support page
Symantec Connect	An online magazine that contains best practices, tips, tricks, and articles for users of this product.	Symantec Connect page